IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 15-CR-182-JHP**
	)	
SCOTT FREDRICK ARTERBURY,	)	
	)	
Defendant.	)	

REPORT AND RECOMMENDATION

Before the Court is the Motion to Suppress Evidence Seized from Residence ("Motion to Suppress") and Request for an Evidentiary Hearing of Defendant Scott Fredrick Arterbury ("Arterbury"). [Dkt. No. 33]. On March 23, 2016, the matter was referred to the undersigned United States Magistrate Judge for Report and Recommendation on the Motion to Suppress. [Dkt. No. 35]. The Motion for hearing has been **GRANTED**, and a hearing conducted on April 25, 2016. After considering the submissions of the parties and the arguments of counsel, the undersigned makes the following findings and recommendation to the District Court.

I.
FACTUAL BACKGROUND – THE "DARK NET" OR TOR

This case involves what is known as the "The Dark Net," the "Tor Network" or "Tor" for short.[1] "Tor is an open-source tool that aims to provide

[1] The Dark Net generally refers to "an area of the Internet only accessible by using an encryption tool called The Onion Router (Tor). Tor is a tool aimed at those desiring privacy online, although frequently attracting those with criminal intentions." Gareth Owen and Nick Savage, "The Tor Dark Net", at 1

anonymity and privacy to those using the Internet. It prevents someone who is observing the user from identifying which sites they are visiting and it prevents sites from identifying the user. Some users value Tor's anonymity because it makes it difficult for governments to censor sites or content that may be hosted elsewhere in the world." Owen and Savage, at 1. An individual living under a repressive government such as North Korea, for example, might make use of Tor to access or post certain information while avoiding government surveillance. However, after analyzing Tor Dark net sites over a six-month period, Owen and Savage found that "the majority of sites were criminally oriented, with drug marketplaces featuring prominently. Notably, however, it was found that sites hosting child abuse imagery were the most frequently requested." *Id.*

The Tor network is designed to route communications through multiple computers, protecting the confidentiality of Internet Protocol ("IP") addresses and other identifying information. *See*, Keith D. Watson, *The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*, 11 Wash. U. Global Stud. L. Rev. 715 (2012) (hereafter, "Watson"). *See, for example*, *U.S. v. Frater*, 2016 WL 795839, *3 (D. Ariz. March 1, 2016).

> Tor allows users to send data over the Internet anonymously by shielding the source's location. This is accomplished by a complex encryption network that dissociates Internet communication from its source's IP address. Tor achieves user anonymity through so-called "onion routing," which bounces all communications routed through the Tor network to various different "nodes" before delivering them to their destination. These "nodes" are proxy

---

[Centre for International Governance Innovation and Royal Institute of International Affairs, September 2015) (hereafter, "Owen & Savage").

> servers scattered across the globe. Tor users connect to the network by first pulling in a list of nodes from a directory server. The user's computer then accesses the Tor network through a random node. The user's information is then routed through a random series of relay nodes before finally routing to an exit node, which sends the user's information to the actual Internet. What is significant about the Tor network is that each node communicates only with the nodes immediately preceding and following it in the chain. Therefore, the user's computer has direct contact with only the first node in the chain, and the actual Internet communicates only with the exit node. The entry node does not know the ultimate destination of the data, and the exit node is unaware of the data's origin. Because exit nodes are the only nodes that communicate directly with the public Internet, any traffic routed through the Tor network is traceable only to the exit node. Each communication is encrypted in a new layer of code before passing to the next node. The communication is eventually ensconced in several layers of code, which are then "peeled away" by the exit node, hence the onion metaphor.
>
> Thus, Computer A submits data through the Tor network, the communication will pass through the network and exit onto the actual Internet through the exit node, Computer B. Any data sent by Computer A will appear to anyone tracing the communication as if it has come from Computer B. This essentially allows the user of Computer A to surf the Internet with complete anonymity, assuming the user never submits any information that is linked to her identity, such as accessing her standard e-mail account.

Watson, at 721-23.

To combat illegal activity using the Tor network, the Government has developed so-called "Trojan horse devices." These may include: "data extraction software, network investigative technique, port reader, harvesting program, remote search, CIPAV for Computer and Internet Protocol Address Verifier, or IPAV for Internet Protocol Address Verifier." Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 Akron L. Rev. 315, 316 (2015). In the instant case, the parties have referred to the warrant issued by the U.S. magistrate judge in the Eastern District of Virginia as a Network

Investigative Technique ("NIT") warrant, and the Court will adopt that terminology.

Once approved, the NIT is installed on the target Website. "Once installed on Website A, each time a user accessed any page of Website A, the NIT sent one or more communications to the user's computer which caused the receiving computer to deliver data to a computer controlled by the FBI, which would help identify the computer which was accessing Website A." *U.S. v. Pierce*, 2014 WL 5173035, *3 (D.Neb. Oct. 14, 2014). In some cases, the Government has even activated a target computer's built-in camera to take photographs of the persons using that computer and send the photos back to the Government. *E.g.*, *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013).

The critical point is that without the use of such techniques as NIT, agents seeking to track a Tor user to his home computer will not be able to take that pursuit beyond the exit node from which the Tor user accessed the regular Internet.[2] NIT allows the Government to surreptitiously send a message back through the Tor network to the home computer directing it to provide information from which the user may be identified.

---

[2] *See for example*, the Affidavit of Douglas Macfarlane offered in support of the Warrant Application in the Eastern District of Virginia. [Dkt. No. 34-1]. Macfarlane states that because of the Tor Network, "traditional IP identification techniques are not viable." [*Id.*, at ¶ 8]. "An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP back through that Tor exit node IP." [*Id.*].

II.
FACTUAL BACKGROUND OF THIS CASE

The Government obtained evidence regarding Arterbury's alleged criminal conduct through a multi-step process that began in the Fall of 2014. At that time, Agents of the Federal Bureau of Investigation ("FBI") began investigating the Playpen website, a global online forum believed to be hosting users for purposes of distributing and accessing child pornography.[3] In February 2015, agents apprehended the administrator of Playpen in Naples, Fla., took control of the site, and moved it to Virginia. Rather than shut Playpen down immediately, agents decided to allow the site to continue operation for 12 days (February 20, 2015 to March 4, 2015) in the hopes of identifying and prosecuting Playpen users. In furtherance of the investigation, the Government sought to use a Network Investigative Technique that would covertly transmit computer code to Playpen users. That code would direct users' computers to provide investigators with information which could then be used to locate and identify the users. In order to employ the NIT, however, the Government needed to obtain an "NIT search warrant."

In February 2015, a warrant application was prepared and presented to a magistrate judge in the Eastern District of Virginia. Absent the use of the NIT, the Government had no ability to locate and identify users of the Playpen

[3] In affidavits in support for the NIT warrant at issue, as well as various pleadings, the parties refer to "Website A." It is now widely known that Website A refers to the "Playpen," a website offering those who access it the opportunity to view and download child pornography. The Court will refer to Playpen, since the identity of the website has been widely publicized.

website. Special Agent Douglas Macfarlane, in his Affidavit in Support of Application for the NIT Search Warrant, stated:

> Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple computers or "nodes" . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

[Dkt. No. 34-1, Affidavit in Support of Application for Search Warrant, at 28-29, ¶ 31].

On February 20, 2015, U.S. Magistrate Judge Theresa Carroll Buchanan issued the NIT warrant. When users accessed Playpen, the NIT caused data extraction software to be installed on the user's computer – wherever it was located. The computer then sent – without Defendant's knowledge or permission – requested information to a Government-controlled computer.[4] In this way, the Government could determine the identity of the person accessing Playpen – even when that person was using a computer that was located outside the Eastern District of Virginia.

Using NIT, agents determined that a Playpen registrant with the user name "johnnyb5" and an IP address of 70.177.122.133 had logged on to the website from February 20 to March 4, 2015. Agents were able to determine that the IP address was operated by Cox Communications, Inc. Using an administrative subpoena directed at Cox, they secured the name and address of the account holder. This information was included in the affidavit of Special

[4] This information included the IP address of the home computer, its type of operating system, the computer's "Host Name", its active operating system username and its media access control ("MAC") address.

Agent Joseph Cecchini in support of a search warrant application presented to U.S. Magistrate Judge T. Lane Wilson in the Northern District of Oklahoma (the "Oklahoma warrant") on November 2, 2015. *See* 15-mj-196-TLW, [Dkt. 1]. The affidavit supporting the Oklahoma warrant is quite similar to the affidavit supporting the NIT warrant application. However, the Oklahoma warrant details the Defendant's alleged conduct regarding the Playpen website and the information obtained as a result of the NIT.

Judge Wilson issued the search warrant for 1515 S. Nyssa Place, Broken Arrow, Oklahoma. Agents executed the warrant, and located and seized alleged child pornography. Judge Wilson then executed a Criminal Complaint and a warrant for the Defendant's arrest.

Defendant appeared before the undersigned on November 16, 2015, at which time, he was released on conditions of supervision.

Defendant's Motion to Suppress seeks to preclude use of any material discovered through the search of his home, arguing, *inter alia*, that the warrant issued by the magistrate judge in Virginia is fatally flawed, and, thus, taints the Oklahoma warrant.

Plaintiff offers three arguments in support of his Motion to Suppress:

- First, that the magistrate judge in Virginia exceeded her authority under Fed. R. Crim. P. 41 by issuing a warrant for property outside her jurisdiction.

- Second, that the affidavit supporting the NIT warrant application falsely represented that the Playpen home page contained a depiction of "prepubescent females, partially clothed with their legs spread."
- Third, the NIT warrant was overbroad because there was not probable cause to justify a search of all "activating computers" on the mere basis of registering with Playpen.

III.
APPLICABLE LEGAL PRINCIPLES

Clearly, a search occurs within the meaning of the Fourth Amendment when "the Government obtains information by physically intruding on a constitutionally protected area." *U.S. v. Jones*, -- U.S. --, 132 S.Ct. 945, 950 n.3 (2012). However, the Fourth Amendment is not concerned just with "trespassory intrusions" on property. *Id.*, at 954 (Sotomayor, J. concurring). The reach of the Fourth Amendment does not "turn upon the presence or absence of a physical intrusion." *Id.* (*citing Katz v. U.S.*, 389 U.S. 347, 353 (1967). As Justice Sotomayor pointed out in *Jones*, we now have a variety of forms of electronic and other "novel modes" of surveillance that do not depend upon a physical intrusion of one's property. Such is the case presented here, where it may not be entirely clear what "property" is being searched or seized or even where that search or seizure occurred.

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

> describing the place to be searched, and the person or things to be seized.

U.S. Const. amend. IV.

A search occurs "when the Government acquires information by either 'physically intruding' on persons, houses, papers or effects,' 'or otherwise invading an area in which the individual has a reasonable expectation of privacy'." *U.S. v. Scully*, 108 F.Supp.3d 59, 75 (E.D.N.Y. 2015). "A seizure occurs when the Government interferes in some meaningful way with the individual's possession of property." *Id.* (*quoting U.S. v. Ganias*, 755 F.3d 125, 133 (2d Cir. 2014). Pursuant to the Federal Rules of Criminal Procedure, the term "property" includes "documents, books, papers, any other tangible objects, and *information*." Fed. R. Crim. P. 41(a)(2)(A) (emphasis added). The Rule permits seizure of electronic and digital data. "Rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses…" *U.S. v. New York Tel. Co.*, 434 U.S. 159, 170 (1977).

The legality of a search is predicated upon a finding that the warrant authorizing the search comports with constitutional requirements and the provisions of Rule 41 which is "designed to protect the integrity of the federal courts or to govern the conduct of federal officers." *U.S. v. Pennington*, 635 F.2d 1387, 1389 (10th Cir. 1980) (*quoting U.S. v. Millar*, 543 F.2d 1280, 1284 (10th Cir. 1976) and *U.S. v. Sellers*, 483 F.2d 37, 43 (5th Cir. 1973), *cert. denied*, 417 U.S. 908 (1974)).

Rule 41 provides in pertinent part:

Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district … has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge -- in an investigation of domestic terrorism or international terrorism -- with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises – o matter who owns them – of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b)(1)-(5).[5]

If the court finds a violation of Rule 41, this does not automatically mean the evidence seized must be suppressed. "Suppression of evidence … has always been our last resort, not our first impulse." *U.S. v. Leon*, 468 U.S. 897, 907 (1984). The exclusionary rule generates "substantial social costs," which sometimes include setting the guilty free and the dangerous at large. We have therefore been "cautio[us] against expanding" it, and "have repeatedly emphasized that the rule's 'costly toll' upon truth-seeking and law enforcement objectives presents a high obstacle for those urging [its] application," *Pennsylvania Bd. of Probation and Parole v. Scott*, 524 U.S. 357, 364–365 (1998) (internal citations omitted).

IV.
RECENT CASES

Several recent decisions arising from the same facts and circumstances before this Court are instructive. These include: *U.S. v. Michaud*, 2016 WL 337263 (W.D.Wash. Jan. 28, 2016); *U.S. v. Stamper*, Case No. 1:15cr109 (S.D.Ohio Feb. 19, 2016); *U.S. v. Epich*, 2016 WL 953269 (E.D.Wis. March 14, 2016); and, *U.S. v. Levin*, 2016 WL 1589824 (D.Mass. April 20, 106).

All of these cases involve the same "sting" operation that netted Defendant Arterbury. All of the cases involve the NIT warrant that was issued by a magistrate judge in the Eastern District of Virginia. In each case, the NIT warrant sent computer malware to an "activating computer" in a district

[5] Here, the warrant was issued pursuant to Rule 41(b)(1) – requesting a search/seizure of property "located in the Eastern District of Virginia." [Dkt. No. 34-1, at 3].

outside of Virginia. That malware seized control of the defendants' computers and caused them to send identifying information to another Government computer in the Eastern District of Virginia. That identifying information was then used to secure a second warrant from a magistrate judge in the defendant's home district authorizing the search and seizure of the defendant's computer.

All of these four cases found that the NIT warrant violated Fed. R. Crim. P. 41(b). However, in *Michaud* and *Stamper*, the courts held that the violationof Rule 41 was a mere "technical violation" that did not prejudice the defendant. *Stamper* adopted the reasoning of *Michaud* that one has no reasonable expectation of privacy in one's IP address and such information, even when extraordinary means have been taken to secret that information. *Michaud* likened the IP address to an unlisted telephone number and opined that the Government would have ultimately been able to get this information without the NIT process.[6]

Epich is of little assistance to this Court because it is governed by Seventh Circuit law holding that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause…." *U.S. v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008). "The remedy of allowing a defendant to go free based on a violation of Rule41'2 requirements for obtaining a proper search warrant would be 'wildly out of proportion to the

[6] I find this conclusion wholly at odds with the Affidavit submitted in support of the NIT warrant wherein the Government stated that absent use of the NIT, It would be impossible to secure the IP address.

wrong'." *U.S. v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008) (*quoting Cazares-Olivas*, 515 F.3d at 730)).

> In light of *Leon*, it is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Claus of the Fourth Amendment, that would call for suppression. Many remedies may be appropriate for deliberate violations of the rules, but freedom for the offender is not among them.

U.S. v. Trost, 152 F.3d 715, 722 (7th Cir. 1998) (*quoting U.S. v. Hornick*, 815 F.2d 1156, 1158 (7th Cir. 1987)).

The Tenth Circuit does not follow the Seventh Circuit in this regard. In *Krueger*, for example, the Tenth Circuit suppressed evidence on the basis of a Rule 41(b) violation; thus, *Epich* is of little assistance to the Court's analysis.

The remaining case is *Levin*, in which the district court – relying heavily on *Krueger* – found a fundamental jurisdictional defect in issuing the NIT warrant in violation of the provisions of Rule 41(b). Because the NIT warrant was void *ab initio*, the Court held, the good faith exception did not apply and the evidence had to be suppressed.

V
DISCUSSION

Because the undersigned believes that the validity of the NIT warrant issued in Virginia is determinative of the Defendant's motion, the Court has focused its attention on that issue and the coincident suppression/good faith issues.

The Court begins by addressing two preliminary issues. First, the warrant under challenge is the NIT warrant issued in the Eastern District of Virginia. That warrant provided probable cause for the issuance of the second, Oklahoma warrant. The Government admitted at the April 25 hearing, that if the NIT warrant is fatally flawed, there would not be probable cause to support the Oklahoma warrant.

Second, the Court seeks to clarify what "property" was seized pursuant to the NIT warrant. The Government contends that in accessing the Playpen website Arterbury sent "packets of data" into the Eastern District of Virginia, and that this digital or electronic data is the property at issue. The Defendant contends that his home computer was the seized property. Essentially, he contends that the computer was first seized pursuant to the NIT warrant when the government, through malware, entered his home, took control of his computer and "searched" it for private information he had endeavored to keep confidential. Subsequently, the computer was physically seized when agents took it pursuant to the Oklahoma warrant.

The Court holds that the property seized was Arterbury's computer. The Government did not seize the "packets of data" Arterbury sent to the Eastern District of Virginia, because it was unable to do so. Since there was no way to get this data, the Government employed the NIT to seize Arterbury's computer and direct it to provide the identifying information without his knowledge. Had the Government seized Arterbury's encrypted information in the Eastern District of Virginia, and, through some sort of forensic tool, un-encrypted it to

learn his identifying information, the Court would be inclined toward the Government's position, but that is not what happened. The Macfarlane affidavit makes it clear that the Government could not obtain Arterbury's IP address until its malware made its way back to his computer in Oklahoma and directed it to provide information to the Government.

A. The Virginia Judge Lacked Rule 41 Authority to Issue the NIT Warrant.

Defendant contends that the magistrate judge in Virginia lacked authority under Fed. R. Crim. P. 41 to issue a warrant seeking to seize/search property outside her judicial district. Rule 41 provides five grounds authorizing a magistrate judge to issue a warrant. Rule 41(b)(1)-(5). The parties agree that subsections (b)(3) and (b)(5) have no application here. Thus the analysis will be confined to subsections (b)(1), (b)(2) & (b)(4).

Subsection 41(b)(1) does not provide authority for the Virginia warrant because Arterbury's computer was not located in or seized in the Eastern District of Virginia.

The Government argues that subsections (b)(2) & b(4) provide authority for the NIT warrant. The Court disagrees.

Subsection (b)(2) applies where a judge signs a warrant to seize property that is within his/her jurisdiction at the time the warrant is signed, but has been re-located outside that jurisdiction at the time the warrant is actually executed. The Government contends that by electronically reaching into the Eastern District of Virginia, Arterbury brought "property" into that district that was subject to the NIT warrant. The Government argues that the property was

then removed from Virginia to Oklahoma, thus, the NIT warrant comports with subsection (b)(2).

The Court is not persuaded by this argument. The property seized in this instance was Arterbury's computer, which at all relevant times remained in Oklahoma. The NIT warrant allowed the Government to send computer code or data extraction instructions to Arterbury's computer, wherever it was located. The Government "seized" that computer and directed it to send certain information to the Government – all without Arterbury's knowledge or permission. Arterbury's computer was never in the Eastern District of Virginia and subsection (b)(2), therefore, does not apply. Furthermore, even if the property seized was electronic information, that property was not located in the Eastern District of Virginia at the time the warrant was signed. This information only appeared in Virginia *after* the Warrant was signed and executed and the Government seized control of Defendant's computer in Oklahoma.

The Court is also unpersuaded by the Government's argument that the NIT warrant is valid under Rule 41(b)(4) as a "tracking warrant." The NIT did not track Defendant's computer as it moved. In *Michaud*, the district court rejected the Government's argument as applied to the same NIT operation, stating, "If the 'installation' occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because Mr. Michaud never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular

district," and "[i]f the installation occurred on Mr. Michaud's computer, applying the tracking device exception again fails, because Mr. Michaud's computer was never physically located within the Eastern District of Virginia." This Court agrees with *Michaud* in this regard and concludes Subsection 41(b)(4) is not applicable. The NIT warrant was not for the purpose of installing a device that would permit authorities to track the movements of Defendant or his property.

Furthermore, the drafters of Rule 41 knew how to avoid the territorial limit on issuance of warrants when they wished to do so. Rule 41(b)((3) removes the territorial limitation in cases involving domestic or international terrorism. In such cases, a magistrate judge "with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district." Rule 41(b)(3). The drafters of Rule 41 could easily have included child pornography in Rule 41(b)(3) and, thereby, avoided the territorial limitation of Rule 41(b)(1) & (2). They did not do so. The Court can only conclude that they did not intend to remove the territorial limit in cases such as the one before the Court.

Authority to issue warrants exists only insofar as granted by the rules, and no further. Accordingly, just as the court concluded in *Michaud*, this Court finds that the NIT warrant was not authorized by any of the applicable provisions of Rule 41.[7] Thus, the court concludes that the issuance of the

[7] Apparently, the Government is aware of the problem of authorizing NIT warrants under the current Rules of Criminal Procedure. The Department of Justice has proposed amendments to Rule 41 that would resolve this issue.

warrant violated Rule 41(b).[8]

B. The Virginia Judge Lacked Authority Under the Federal Magistrate Judges Act.

There is another fundamental problem with the Virginia magistrate judge's authority to issue the NIT warrant. As Judge Gorsuch noted in his concurring opinion in *Krueger*, the Government's problem goes to the heart of the magistrate judge's statutory source of power. The Federal Magistrate Judges Act provides three territorial limits on a magistrate judge's power:

> Each United States magistrate judge serving under this chapter shall have [1] within the district in which sessions are held by the court that appointed the magistrate judge, [2] at other places where that court may function, and [3] elsewhere as authorized by law … all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts….

Id. at 1118 (*citing* 28 U.S.C. § 636(a)).[9]

As in *Krueger*, the magistrate judge "purported to exercise power in none of these places." 809 F.3d at 1118. Thus, Judge Gorsuch notes, "The warrant on which the government seeks to justify its search in this case was no warrant at all when looking to the statutes of the United States." *Id.* (emphasis added).

---

[8] Defendant also asserts the NIT Warrant lacked statutory jurisdiction and therefore violated the Fourth Amendment. [Dkt. No. 33 at pp. 10-11 (*citing* Judge Gorsuch's concurring opinion in *Krueger*, 809 F.3d at 1117-26)]. However, consistent with the majority opinion in *Krueger*, since the court has determined that there was a clear Rule 41(b) violation, it declines to reach this issue. *Id.* at 1104-05 ("[C]onsistent with the fundamental rule of judicial restraint, we decline to reach a constitutional question that is not necessary for our resolution of this appeal (citation omitted)).

[9] In *Krueger*, the government secured a warrant from a magistrate judge in Kansas permitting the seizure and search of property located in Oklahoma. The Tenth Circuit affirmed the lower court's finding that the warrant violated Rule 41 and the court's suppression of the evidence seized pursuant to the invalid warrant. *See*, discussion at p. 19-21, *infra*.

C. Under *Krueger*, Suppression is Warranted Because the Search Would Not Have Occurred But For the Breach of Rule 41(b).

The court must next consider whether suppression is justified. To establish the case for suppression, Defendant must show that he was prejudiced by the violation of Rule 41. The prejudice standard adopted in *Krueger* allows defendant to show either "(1) prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) intentional disregard for a provision of the Rule." *Krueger*, 809 F.3d at 1115 (citing *United States v. Pennington*, 635 F.2d 1387, 1390 (10th Cir. 1980)). As set forth above, the court does not address whether the warrant fails for constitutional reasons, but limits its analysis to the violation of Rule 41(b). Specifically, does a violation of Rule 41(b) justify suppression of evidence?

In *Krueger*, the Tenth Circuit addressed this question for the first time. ("The Court has not yet had occasion to consider whether suppression is justified when a warrant is issued by a federal magistrate judge who clearly lacks authority to do so under Rule 41(b)(1)." *Krueger*, 809 F.3d at 1115). The court answered that question affirmatively.

In *Krueger*, a Homeland Security Investigations ("HSI") agent learned that child pornography was being distributed over the internet from an IP address registered to Krueger, a Kansas resident. *Id.* at 1111. The agent obtained a warrant ("Warrant 1") from a United States magistrate judge in the District of Kansas to search defendant Krueger's Kansas residence for items such as

computers and cell phones that might be used to depict child pornography. *Id.* Upon executing the warrant, the agent was told by Krueger's roommate that Krueger was in Oklahoma City and may have taken his computer and cell phone with him. *Id.* After an HSI agent in Oklahoma verified Krueger's whereabouts, the agent in Kansas sought and obtained a second warrant ("Warrant 2") from a different magistrate judge in the District of Kansas. *Id.* The second warrant authorized law enforcement to search the Oklahoma residence where Krueger was staying and Krueger's automobile. The warrant was immediately transmitted to an HSI agent in Oklahoma, who executed the warrant and seized Krueger's computer and external hard drive. *Id.* A subsequent search of the devices revealed evidence that Krueger had downloaded and traded child pornography using his peer-to-peer networking account and, as a result, Krueger was charged with distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2). *Id.* at 1112. Krueger filed a motion to suppress, asserting Warrant 2 violated Rule 41(b)(1) because the magistrate judge in the District of Kansas did not have authority to issue a warrant for property already located in Oklahoma. *Id.* After a suppression hearing, the district court granted the motion, concluding that the warrant violated Rule 41(b)(1) and Krueger had demonstrated prejudice in the sense that the Kansas magistrate judge would not have issued Warrant 2 had Rule 41 "been followed to the letter." *Id.* at 1112-13.

On appeal, the Government conceded that Warrant 2 violated Rule 41(b)(1) because the magistrate judge in Kansas had no authority to issue a

warrant for property already located in Oklahoma but argued the district court applied the wrong legal standard in determining that Krueger demonstrated prejudice as a result of the violation. *Id.* at 1113. The Government asserted the appropriate question was not whether any judge in the District of *Kansas* could have issued Warrant 2, but instead was whether any judge in the Western District of *Oklahoma* could had issued the warrant. *Id.* at 1116. The Tenth Circuit disagreed, concluding the Government's proposed approach was too speculative. *Id.* It stated, "[I]nstead of focusing on what the Government *could have* done to comply with Rule 41(b)(1), we conclude that prejudice in this context should be anchored to the facts as they actually occurred." *Id.* Accordingly, it adopted the district court's standard for determining whether defendant had established prejudice and asked "whether the issuing federal magistrate judge could have complied with the Rule." *Id.*

The Government argues *Krueger* is inapposite because there, the agent knew the exact location of the evidence being sought, and was aware the location was in Oklahoma, when he obtained Warrant 2 from a Kansas magistrate judge. Here, in contrast, the agent did not know and could not have known the physical location of Playpen registrants due to the affirmative steps taken by Playpen administrators and users to conceal their illegal activity.

The Government's position finds some support in *Michaud*, *supra*. In *Michaud*, the district court concluded that although a technical violation of Rule 41 had occurred, suppression was not warranted because the record did

not show that defendant was prejudiced or that the FBI acted intentionally and with deliberate disregard of Rule 41(b). Applying the Ninth Circuit's definition of prejudice, i.e., "prejudice 'in the sense that the **search** would not have occurred . . . if the rule had been followed,'" the district court found that the defendant had "no reasonable expectation of privacy of the most significant information gathered by deployment of the **NIT**, Mr. Michaud's assigned IP address, which ultimately led to Mr. Michaud's geographic location." *Id.* at **6-7. Furthermore, the court concluded that "[t]he IP address was public information, like an unlisted telephone number, and eventually could have been discovered." *Id.* at *7.[10]

The Tenth Circuit's definition of "prejudice" – *i.e.*, "prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed" – is similar to the Ninth Circuit definition. *See Krueger*, 809 F.3d at 1115. Here, the searches of Arterbury's computer would not have occurred had Rule 41(b) been followed. Absent deployment of the NIT, the physical location of Playpen registrants was not discoverable. *See Macfarlane Affidavit*, Dkt. No. 34-1]. Under the *Krueger/Pennington* framework, the evidence must be suppressed. Rule 41 was clearly violated, and the Oklahoma search would not have occurred had Rule 41(b) been

[10] The court in *Michaud* offered no citation or support for these conclusions. The court indicated that the Government would have no difficulty discovering the IP address for an individual using the Tor network. This is contrary to the undersigned's understanding of how the Tor network works and is specifically contradicted by the statements set forth in Special Agent Macfarlane's Affidavit seeking the NIT Warrant in the Eastern District of Virginia. [Dkt. No. 34-1, ¶¶ 8, 9, & 31].

followed. Furthermore, *Krueger* articulates the appropriate inquiry as whether any magistrate judge in the Eastern District of Virginia could have complied with Rule 41 given the facts of this case. The answer to that question is "no."

The Government also argues that there was no prejudice to Arterbury because he had no reasonable expectation of privacy in his IP address. The Government asserts that the IP address is actually the property of the Internet Service Provider, and that one must disclose this IP address to a third-party in order to access the Internet. Were the IP address obtained from a third-party, the Court might have sympathy for this position. However, here the IP address was obtained through use of computer malware that entered Defendant's home, seized his computer and directed it to provide information that the Macfarlane affidavit states was unobtainable in any other way. Defendant endeavored to maintain the confidentiality of his IP address, and had an expectation that the Government would not surreptitiously enter his home and secure the information from his computer.

D. The "Good Faith Exception Does Not Apply.

The most troubling aspect of this case is whether suppression of evidence can be avoided through application of the "good-faith" exception to the exclusionary rule. Having determined that the NIT warrant was void as against Aterbury, the Court must determine whether suppression of the evidence found during the search of his home is warranted. In *U.S. v. Leon*, 468 U.S. 897 (1984), and its companion case, *Mass. v. Sheppard*, 468 U.S. 981 (1984), the Supreme Court recognized a "good faith" or *Leon* exception to the Fourth

Amendment exclusionary rule.[11] Under the *Leon* exception, evidence obtained pursuant to a warrant later found to be invalid may be introduced in the government's case-in-chief at the defendant's trial, if a reasonably well-trained officer would have believed that the warrant was valid. The premise for the exception is that there is inadequate justification to apply the exclusionary rule when police obtain a warrant, reasonably relying on its validity, only to later learn that the judge erred in authorizing the search. The court noted in *Leon*, "Penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Leon*, 468 U.S. at 921.

In *Krueger*, the Tenth Circuit held that violation of Rule 41(b) justified suppression of evidence; however, *Krueger* dealt with a single warrant – a warrant issued by a Kansas magistrate judge authorizing search and seizure of property in Oklahoma. This case – and those cited above in ¶IV – presents a different scenario: a second warrant is secured in the appropriate jurisdiction, but probable cause for the second warrant was secured by means of an earlier, invalid warrant. Should the good-faith exception permit officers to rely on the second, valid warrant? Or is the second warrant fatally flawed because of the invalidity of the first warrant?

---

[11] *Leon* "contemplated two circumstances: one in which a warrant is issued and is subsequently found to be unsupported by probably cause and the other in which a warrant is supported by probable cause, but is technically deficient." *U.S. v. Levin*, 2016 WL 1589824 (D.Mass. April 20, 2016) (*quoting U.S. v. Vinnie*, 683 F.Supp. 285, 288 (D. Mass. 1988)).

The Government first contends that the *Leon* exception should apply here because the NIT warrant is a "technical violation" of Rule 41(b). The Court rejects the notion that this case presents nothing more than a "technical violation" of Rule 41. It is true that courts have found that suppression is not warranted in some cases of a Rule 41 violation; however, these have generally involved violations of procedural requirements under Rule 41(a), (c), (d), or (e). *E.g.*, *U.S. v. Rome*, 809 F.2d 665 (10th Cir. 1987) (violation of Rule 41(c)). *See Krueger*, 809 F.3d at 1115, n.7 (collecting cases). However, in this case the violation of Rule 41 goes to the fundamental jurisdiction and "substantive judicial authority" of the magistrate judge to issue the NIT warrant. *Krueger*, 809 F.3d at 1115, n.7 (*citing Berkos*, 543 F.3d at 397).

In *Levin*, the Court relied on *Krueger* and *Berkos* to distinguish technical violations of Rule 41 from the type of violation presented here:

> Rule 41, however, has both procedural and substantive provisions — and the difference matters. Courts faced with violations of Rule 41's procedural requirements have generally found such violations to be merely ministerial or technical, and as a result have determined suppression to be unwarranted. By contrast, this case involves a violation of Rule 41(b), which is "a substantive provision[.]" *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008); *see also United States v. Krueger*, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015) (noting that Rule 41(b)(1) "is unique from other provisions of Rule 41 because it implicates substantive judicial authority," and accordingly concluding that past cases involving violations of other subsections of Rule 41 "offer limited guidance") (internal quotation marks and citation omitted). Thus, it does not follow from cases involving violations of Rule 41's procedural provisions that the Rule 41(b) violation at issue here — which involves the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the warrant — was simply ministerial. *See United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013) (concluding that a Rule 41(b) violation constitutes

> a "jurisdictional flaw" that cannot "be excused as a 'technical defect"').

Levin, 2016 WL 1589824, at *7

In *Krueger*, the trial Court noted, "[I]t is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by 'good faith.' " *U.S. v. Krueger*, 998 F.Supp.2d 1032, 1036 (D.Kan. 2014) (*quoting U.S. v. Glover*, 736 F.3d 509, 516 (D.C.Cir. 2013)).

Levin concluded that the good-faith exception was inapplicable to a warrant held to be void *ab initio* under Rule 41(b). *Id.* Other courts have indicated, in dicta, that where evidence is obtained pursuant to a warrant that is void *ab initio*, the good-faith exception does not apply. *See*, *Levin*, at *10 & n.17 (collecting cases). *See also*, *State v. Wilson*, 618 N.W.2d 513, 520 (S.D. 2000) (good-faith exception inapplicable to warrant by state judge acting outside territorial jurisdiction); *State v. Nunez*, 634 A.2d 1167, 1171 (D.R.I. 1993) (good faith exception would not apply to a warrant that is void *ab initio*).

Based on the holdings of *Krueger* and *Levin*, I conclude that where the Rule 41 violation goes directly to the magistrate judge's fundamental authority to issue the warrant, as in the violation presented here, it is not a "technical violation" of the Rule. The warrant is void *ab initio*, suppression is warranted and the good-faith exception is inapplicable.

The Government also argues that because of exigent circumstances the NIT search would have been justified, even had the magistrate judge in Virginia refused to sign it. The Court is not persuaded by this argument either. The

exigent circumstances were the on-going downloading and distribution of child pornography. In this instance, the specific activity at issue was on-going only because the Government opted to keep the Playpen site operating while it employed the NIT. The Government cannot assert exigent circumstances when it had a hand in creating the emergency.

Exclusion of the evidence in this case will serve the remedial and prophylactic purposes of the exclusionary rule, by serving notice to the Government that use of an NIT warrant under the circumstances presented here exceeds a magistrate judge's authority under the Federal Magistrate Judges Act and Rule 41(b) of the Rules of Criminal Procedure.

The NIT Warrant clearly did not comport with Fed. R. Crim. P. 41(b), and, therefore, was invalid *ab initio*. Arterbury was prejudiced by issuance of the NIT Warrant and the Court finds no basis for application of the good faith exception to the exclusionary rule. Accordingly, Defendant's motion to suppress [Dkt. No. 33] must be granted.[12]

V.
CONCLUSION

The purpose of Rule 41 is to carry out the mandate of the Fourth Amendment. It binds federal courts and federal law enforcement officers. *Navarro v. U.S.*, 400 F.2d 315, 318-19 (5th Cir 1968), *overruled on other grounds*, *U.S. v. McKeever*, 905 F.2d 829, 833 (5th Cir. 1990)):

[12] Having determined the United States magistrate judge in Virginia exceeded her authority under Fed. R. Crim. P. 41, the court declines to address defendant's remaining arguments in support of suppression.

> The obligation of the federal agent is to obey the Rules. They are drawn for the innocent and guilty alike. They prescribe standards for law enforcement. They are designed to protect the privacy of the citizen, unless the strict standards set for searches and seizures are satisfied. That policy is defeated if the federal agent can flout them and use the fruits of his unlawful act either in federal or state proceedings.

Rea v. United States, 350 U.S. 214, 217-18 (1956).

- The NIT warrant was issued in violation of Rule 41(b).
- The violation was not a "technical violation" because it implicates "substantive judicial authority." *Krueger*, 809 F.3d at 1115, n.7.
- The NIT warrant was, therefore, void *ab initio*. *Levin*, at *8.
- The *Leon* exception does not apply when an underlying warrant is void *ab initio*. *Levin*, at *11-*12.

Accordingly, for the reasons set forth above, I recommend the Defendant's Motion to Suppress [Dkt. No. 33] be **GRANTED**.

OBJECTIONS

The District Judge assigned to this case will conduct a de novo review of the record and determine whether to adopt or revise this Report and Recommendation or whether to recommit the matter to the undersigned. As part of his/her review of the record, the District Judge will consider the parties' written objections to this Report and Recommendation. In order to expedite this matter for consideration by the District Judge, the period for objections must be shortened. *See* Fed. R. Crim P. 59(b). Therefore, a party wishing to file objections to this Report and Recommendation must do so **by May 2, 2016**. *See* 28 U.S.C. § 636(b)(1) and Fed. R. Crim. P. 59(b). The failure to file timely

written objections to this Report and Recommendation waives a party's right to review. Fed. R. Crim P. 59(b).

DATED this 25th day of April 2016.

Paul J. Cleary
United States Magistrate Judge